4.5 Saving Electronic PHI

1. **Do Not Save PHI to Local Computer**—Do not save any PHI or other sensitive data to your local computer (C: or D: drives). Sensitive data, including PHI, should be saved to a local secure account file share.

2. **Saving PHI to Network File Share**—When saving sensitive data to a network file share, be sure to save it in the appropriate location. For example, do not save a fax of a member's medical records in a folder to which all employees have access.

3. **Saving PHI to Removable Data Device**—If it is necessary to save sensitive data to a CD, thumb drive, or other removable data device, use encryption and password-protection methods. For example, put the sensitive documents in a WinZip file and password-protect it, which also encrypts it.

4.6 Personally Transporting of PHI

1. **Transporting PHI**—When personally transporting PHI (or preparing it to go) outside the building, be sure it is carried in a locked container and is double-bagged. When delivering it to someone who is not in an office-type facility, be sure you've given them advance notice so that they can bring appropriate secured containers with them to receive the information. It is not our responsibility to ensure that they do so, but we are obligated to give them the opportunity.

2. **Lockable Containers**—Options for lockable containers include suitcases, laptop bags, plastic totes, and so forth. A lock can be either a key lock or the plastic zip-ties that are not re-usable.

4.7 Connecting to HP Enterprise Services From Home or Off-Site Locations

Ensure that you use the HP Enterprise Services-approved communication methods for accessing HP Enterprise Services resources and applications.

Always use HP Enterprise Services computer equipment to perform your work. Access to HP ES is not permitted from non-HP Enterprise Services computer.

4.8 Security of Your Computer

If you have a laptop, be sure to either physically lock it in an overhead bin, file cabinet, or other secured location at the end of the day or bring it home with you. When traveling and/or during your daily commute, take appropriate measures to protect it. An example would be to lock your laptop in the trunk of your car when leaving your car unattended.

When leaving your desk for any reason or for any amount of time, always lock your workstation to prevent others from using it. This is accomplished by either pressing the Ctrl-Alt-Delete keys, or by pressing the Windows key and L simultaneously.

Follow all HP Enterprise Services corporate and the HP Enterprise Services GAMMIS directives regarding the rollout of encryption tools.

If your HP-issued IT asset is lost or stolen, you must complete the following steps immediately, depending on the asset:

1. Required steps for all lost/stolen IT assets:

    a. File a lost/stolen report with local law enforcement. Obtain a report number, and the name and phone number of the reporting officer of the law enforcement agency.

    b. Report the incident to the Corporate IT Security Incident Response Team (CITSIRT) by completing this form.

2. Required steps for lost/stolen PCs (laptops or desktops):

    a. All PCs which have been Lost or Stolen must be reported to the Corporate IT Security Incident Response Team (CITSIRT). You will receive an incident number which will be required to validate your PC replacement request.

    b. Reset the password for your domain account. Note: Reset passwords for all other accounts which may have been compromised.

    c. Update the PC Status for your lost/stolen PC by completing this form.

    d. Report the matter to your manager. If approved by your manager, order a replacement PC. Click here for details about requesting a new PC.

3. Required steps for lost/stolen phones:

    a. If a phone was lost or stolen and has HP's Managed Mobility Services (MMS) software installed on it, you must perform a remote wipe of the data by using the MMS self care tool.

4.9 Disposal of PHI

Use the recycle bins to dispose of all PHI or other sensitive information, as the contents are shredded. If the information is extremely sensitive and you'd prefer to shred it yourself, contact the administrative team to locate one of the shredders nearest to you. Under no circumstance should PHI or other sensitive documentation be discarded in the regular trashcans.

If you need to dispose of PHI on electronic media, like a CD or diskette, contact the Network team or the HIPAA privacy officer to determine the appropriate destruction method.

Note: Dispose of all PHI at an HP Enterprise Services location unless discussed otherwise with your team leader.

4 Responsiveness and Recovery Scenarios

4.1 Backup Strategy

The protection of GAMMIS records and documentation is of the utmost importance to the HP Enterprise Services system support staff. The backup jobs are scheduled to begin running at 6:00 p.m. Eastern Standard Time, Monday to Friday and throughout the day on Saturday and Sunday. Backups cover all partitions on each respective server. Backups are taken from the primary disks to tape (disk-to-tape). This strategy insures that the most recent backups are always available for recovery, if needed. When each backup reaches tape, that tape is kept onsite with a copy sent offsite. These offsite copies are encrypted to meet HIPAA requirements, and will stay offsite based on the tape rotation scheme. The offsite tape storage facility provides a comparable level of security including file, sabotage, and environmental considerations. HP Enterprise Services maintains a media refresh policy to copy stored data on a regular basis to limit the inherent degradation of magnetic media.

Example -

Server/Database	**Type of backup**
Unix Servers	Incremental –daily (cumulative) Full – weekly Friday
Windows Servers	Full –daily
Database (SQL)	Full - daily
Database (Oracle)	Incremental – daily Full - weekly
Voice platform including Interactive Voice Response System (IVRS)	Incremental –daily Full - weekly/monthly
Imaging/Data Entry	Incremental –daily Full – weekly/monthly

The tape rotation is based on the frequency listed in the above table. The rotation schedule is defined in Tape Backup Rotation Scheme section in chapter 4.

The HIPPA and DOD approved encryption used for tape backup utilizes a double key methodology. An initial "key set" is created during the implementation process. This key set must be